IN THE CLAIMS:

Please **CANCEL** claims 11-12 and 21-22 without prejudice or disclaimer.

Please **AMEND** claims 1-5, 8, 10, 13-15, and 17-20 as follows.

Please **ADD** claims 23-69 as follows.

1. (Currently Amended) A method, comprising: ~~for authenticating a terminal in a communication system, the terminal comprising identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key; the method comprising;~~

executing ~~a second~~ an authentication protocol, wherein the terminal authentication protocol comprises~~authenticates the~~

authenticating an identity of a network entity ~~and the~~ by a terminal in a communication system;

sharing a ~~and the network entity share a second~~ key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and ~~and subsequently~~

executing ~~a third~~ another authentication protocol comprising~~by the steps of:~~

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by ~~at least~~ applying ~~one of the~~ an authentication function ~~functions~~ to the challenge data~~, by means of the identification means;~~

~~transmitting~~ sending a message comprising terminal authentication data, from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service~~,~~;

wherein ~~in~~ the determining ~~step the terminal is provided~~ comprises providing the terminal with access to the service only ~~if~~ when the terminal authentication data equals a predetermined function of at least the test data and the ~~second~~ key.

2. (Currently Amended) A method as claimed in claim 1, ~~wherein the method comprises:~~further comprising:

forming the test data by applying the authentication function to the challenge data at the authentication functionality; and

~~transmitting~~ sending the test data from the authentication functionality to the network entity,~~;~~

~~and~~

wherein the determining ~~step~~ comprises forming network authentication data by applying the predetermined function to the test data and the key at the network entity,~~;~~ and

wherein ~~in~~ the determining ~~step~~ further comprises providing the terminal ~~is provided~~ with access to the service only ~~if~~ when the terminal authentication data equals the network authentication data.

3. (Currently Amended) A method as claimed in claim 1, ~~wherein the method comprises:~~ further comprising:

~~transmitting~~ sending the ~~second~~ key from the network entity to the authentication functionality;

forming the test data by applying the authentication function to the challenge data at the authentication functionality; and

forming network authentication data by applying the predetermined function to the test data and the key at the authentication functionality.

4. (Currently Amended) A method as claimed in claim 3, further comprising:

~~transmitting~~ sending the terminal authentication data from the network entity to the authentication functionality; and

~~transmitting~~sending, from the authentication functionality to the network entity, an indication of whether the terminal authentication data equals the network authentication data,~~;~~

~~and~~

wherein ~~in~~ the determining ~~step~~ comprises providing the terminal ~~is provided~~ with access to the service only ~~if~~ when the indication is that the terminal authentication data equals the network authentication data.

5. (Currently Amended) A method as claimed in claim 3, further comprising:

~~transmitting~~ sending the network authentication data from the authentication functionality to the network entity,~~;~~

~~and~~

wherein ~~in~~ the determining ~~step~~ comprises providing the terminal ~~is provided~~ with access to the service only ~~if~~ when the indication is that the terminal authentication data equals the network authentication data.

6. (Previously Presented) A method as claimed in claim 1, wherein the terminal authentication data is formed as a cryptographic checksum.

7. (Previously Presented) A method as claimed in claim 1, wherein the network entity is co-located with the authentication functionality.

8. (Currently Amended) A method as claimed in claim 1, wherein ~~authentication means is~~ an identity module of the terminal is configured to perform the authentication function.

9. (Original) A method as claimed in claim 8, wherein the identity module is user-removable from the terminal.

10. (Currently Amended) A method as claimed in claim 8, wherein the identity module is a ~~SIM~~ subscriber identity module or a ~~USIM~~universal subscriber identity module.

11-12. (Cancelled)

13. (Currently Amended) A method as claimed in claim ~~1~~8, wherein the ~~authentication means stores~~identity module is configured to store a code and the authentication function comprises ~~applying~~ a cryptographic transformation applied to the code and the input data.

14. (Currently Amended) A method as claimed in claim 1, wherein the ~~second~~ authentication protocol is ~~the~~ one of a pre-internet key exchange credential provisioning protocol~~PIC~~, ~~the PEAP~~ a protected extensible authentication protocol, or ~~the EAP-TTLS~~ an extensible authentication protocol-tunneled transport layer security.

15. (Currently Amended) A method as claimed in claim 1, wherein the challenge data and the response data are formed according to ~~the EAP~~an extensible authentication protocol.

16. (Previously Presented) A method as claimed in claim 1, wherein the said message is a dedicated authentication message.

17. (Currently Amended) A method as claimed in claim 1, wherein the predetermined function is used for derivation of a session key to be used for one of encryption ~~and/~~or authentication of communications between the terminal and the network entity.

18. (Currently Amended) A ~~communication~~ system, comprising:

a terminal configured to apply authentication functions to input data to form response data; and

a network entity configured to provide access to a service,

wherein the system is configured to perform an authentication method of executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of the network entity by the terminal in the system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service;

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

~~identification means for applying authentication functions to input data to form response data, and the communication system being arranged to utilise a first authentication protocol for authentication of the terminal, wherein an authentication~~

~~functionality and the terminal share challenge data, the terminal forms response data and a first key by applying the authentication functions to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data and can apply an authentication function to the challenge data to duplicate the first key; the system being arranged to perform an authentication method comprising the steps of: executing a second authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a second key for use in securing subsequent communications between the terminal and the network entity; and subsequently executing a third authentication protocol by the steps of:~~

~~sharing challenge data between the network entity and the terminal;~~

~~forming at the terminal test data by at least applying one of the authentication functions to the challenge data by means of the identification means;~~

~~transmitting a message comprising terminal authentication data, from the terminal to the network entity;~~

~~and determining based on the terminal authentication data whether to provide the terminal with access to a service;~~

~~wherein in the determining step the terminal is provided with access to the service only if the terminal authentication data is consistent with the network authentication data computed as a predetermined function of at least the test data and the second key.~~

19. (Currently Amended) A ~~communication~~ system as claimed in claim 18, wherein the system is further configured to execute a linking protocol by forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol, and forming at the network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol,

wherein the secret session keys are configured to secure the subsequent communications between the terminal and some network element. ~~comprising~~

~~a terminal, a network entity and an authentication functionality, the terminal comprising identification means for applying an authentication function to input data to form response data, and the communication system being arranged to utilise a first authentication protocol wherein the terminal authenticates the identity of a network entity and the terminal and the network entity share a key for use in securing subsequent communications between the terminal and the network entity; and the communication system being arranged to perform an authentication method comprising the steps of: executing a second authentication protocol for authentication of the terminal,~~

~~wherein an authentication functionality supplies challenge data to the terminal, the terminal forms response data and test data by applying the authentication function to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data; and subsequently executing a third linking~~

~~protocol by the steps of forming at the terminal secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; forming at the network entity secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; wherein in the secret session keys are used to secure the subsequent communication between the terminal and some network element.~~

20. (Currently Amended) A ~~an authentication~~ method as claimed in claim 1, further comprising:

forming at the terminal secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol; and

forming at the network entity secret session keys by at least applying a predetermined function to the test data using the shared key established in the another authentication protocol,

wherein the secret session keys are configured to secure the subsequent communications between the terminal and a network element.

~~for use in a communication system comprising a terminal, a network entity and an authentication functionality, the terminal comprising identification means for applying an authentication function to input data to form response data, and the communication system being arranged to utilise a first authentication protocolwherein the terminal~~

~~authenticates the identity of a network entity and the terminal and the network entity share a key for use in securing subsequent communications between the terminal and the network entity; and the authentication method comprising the steps of: executing a second authentication protocol for authentication of the terminal, wherein an authentication functionality supplies challenge data to the terminal, the terminal forms response data and test data by applying the authentication function to the challenge data by means of the identification means, and returns the response data to the authentication functionality, and the authentication functionality authenticates the terminal by means of the response data; and subsequently executing a third linking protocol by the steps of forming at the terminal secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; forming at the network entity secret session keys by at least applying a predetermined function to the secret test data by means of the shared key established in the first protocol; wherein in the secret session keys are used to secure the subsequent communication between the terminal and some network element.~~

21-22. (Cancelled)

23. (New) A method as claimed in claim 1, further comprising:

executing a third authentication protocol for authentication of the terminal comprising:

sharing between an authentication functionality and the challenge data;

forming response data and another key at the terminal by applying the authentication function to the challenge data;

sending the response data to the authentication functionality from the terminal;

authenticating the terminal at the authentication functionality using the response data; and

applying the authentication function to the challenge data to duplicate the another key.

24. (New) A method as claimed in claim 23, wherein the third authentication protocol is an authentication and key agreement protocol or any protocol of the extensible authentication protocol family.

25. (New) A method as claimed in claim 24, wherein the test data comprises one or both of an authentication and key agreement protocol integrity key value or an authentication and key agreement protocol cipher key value.

26. (New) A method, comprising:

executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

receiving a key at the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the terminal key.

27. (New) A method as claimed in claim 26, wherein the terminal authentication data is formed as a cryptographic checksum

28. (New) A method as claimed in claim 26, wherein the network entity is co-located with the authentication functionality.

29. (New) A method as claimed in claim 26, wherein an identity module of the terminal is configured to perform the authentication function.

30. (New) A method as claimed in claim 29, wherein the identity module is user-removable from the terminal.

31. (New) A method as claimed in claim 29, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

32. (New) A method as claimed in claim 29, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

33. (New) A method as claimed in claim 26, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

34. (New) A method as claimed in claim 26, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

35. (New) A method as claimed in claim 26, wherein the message is a dedicated authentication message.

36. (New) A method, comprising:

executing an authentication protocol, wherein the authentication protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system;

sending a key to the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data from the terminal at the network entity;

determining, based on the terminal authentication data, whether to provide the terminal with access to a service; and

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

37. (New) A method as claimed in claim 36, wherein the terminal authentication data is formed as a cryptographic checksum.

38. (New) A method as claimed in claim 36, wherein the network entity is co-located with the authentication functionality.

39. (New) A method as claimed in claim 36, wherein an identity module of the terminal is configured to perform the authentication function.

40. (New) A method as claimed in claim 39, wherein the identity module is user-removable from the terminal.

41. (New) A method as claimed in claim 39, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

42. (New) A method as claimed in claim 39, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

43. (New) A method as claimed in claim 36, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

44. (New) A method as claimed in claim 36, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

45. (New) A method as claimed in claim 36, wherein the message is a dedicated authentication message.

46. (New) A method as claimed in claim 36, wherein the predetermined function is used for derivation of a session key to be used for one of encryption or authentication of the subsequent communications between the terminal and the network entity.

47. (New) An apparatus, comprising:

a processor configured to apply an authentication function to input data to form response data, and to execute an authentication protocol,

wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

receiving a key at the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity;

wherein the processor is further configured to execute another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the key.

48. (New) An apparatus as claimed in claim 47, wherein the terminal authentication data is formed as a cryptographic checksum.

49. (New) An apparatus as claimed in claim 47, wherein the network entity is co-located with the authentication functionality.

50. (New) An apparatus as claimed in claim 47, wherein an identity module of the terminal is configured to perform the authentication function.

51. (New) An apparatus as claimed in claim 50, wherein the identity module is user-removable from the terminal.

52. (New) An apparatus as claimed in claim 50, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

53. (New) An apparatus as claimed in claim 50, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

54. (New) An apparatus as claimed in claim 47, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

55. (New) An apparatus as claimed in claim 47, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

56. (New) An apparatus as claimed in claim 47, wherein the message is a dedicated authentication message.

57. (New) An apparatus, comprising:

a processor configured to execute an authentication protocol, wherein the authentication protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system; and

sending a key to the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity;

wherein the processor is further configured to execute another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data, from the terminal at the network entity;

determining, based on the terminal authentication data, whether to provide the terminal with access to a service; and

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

58. (New) An apparatus as claimed in claim 57, wherein the terminal authentication data is formed as a cryptographic checksum.

59. (New) An apparatus as claimed in claim 57, wherein the network entity is co-located with the authentication functionality.

60. (New) An apparatus as claimed in claim 57, wherein an identity module of the terminal is configured to perform the authentication function.

61. (New) An apparatus as claimed in claim 60, wherein the identity module is user-removable from the terminal.

62. (New) An apparatus as claimed in claim 60, wherein the identity module is a subscriber identity module or a universal subscriber identity module.

63. (New) An apparatus as claimed in claim 60, wherein the identity module is configured to store a code and the authentication function comprises a cryptographic transformation applied to the code and the input data.

64. (New) An apparatus as claimed in claim 57, wherein the authentication protocol is one of a pre-internet key exchange credential provisioning protocol, a protected extensible authentication protocol or an extensible authentication protocol-tunneled transport layer security.

65. (New) An apparatus as claimed in claim 57, wherein the challenge data and the response data are formed according to an extensible authentication protocol.

66. (New) An apparatus as claimed in claim 57, wherein the message is a dedicated authentication message.

67. (New) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a method comprising:

executing an authentication protocol, wherein the terminal authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system;

sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sharing challenge data between the network entity and the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data, from the terminal to the network entity; and

determining, based on the terminal authentication data, whether to provide the terminal with access to a service,

wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

68. (New) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a method comprising:

executing an authentication protocol, wherein the authentication protocol comprises

authenticating an identity of a network entity by a terminal in a communication system, and

receiving a key at the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

receiving challenge data from the network entity at the terminal;

forming at the terminal test data by applying an authentication function to the challenge data;

sending a message comprising terminal authentication data from the terminal to the network entity; and

receiving access to a service at the terminal following a determination of whether the terminal authentication data equals a predetermined function of at least the test data and the terminal key.

69. (New) A computer program product embodied on a computer readable storage medium, the computer program product being configured to control a processor to perform a method comprising:

executing an authentication protocol, wherein the authentication protocol comprises

sending an identity of a network entity for authentication by a terminal in a communication system;

sending a key to the terminal from the network entity for use in securing subsequent communications between the terminal and the network entity; and

executing another authentication protocol comprising

sending challenge data from the network entity to the terminal for forming test data at the terminal by applying an authentication function to the challenge data;

receiving a message comprising terminal authentication data from the terminal at the network entity;

determining, based on the terminal authentication data, whether to provide the terminal with access to a service; and

providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.